Appln. No. 09/772,460
Amendment dated: November 8, 2004
Reply to Office Action of August 6, 2004

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended):   An electronic downloading A system for securely downloading encrypted electronic information from a host device to a gaming terminal of an electronic gaming system through a communications link between said host device and said terminal, wherein said terminal comprises a decryption component configured for decrypting, said encrypted electronic information being encrypted by using at least two security keys, and wherein at least a first one said key being of said security keys is resident in said terminal and at least another said a second key of said security keys is non-resident in said terminal and separately delivered to said terminal apart from said encrypted electronic information being delivered to said terminal at the time of said downloading, and wherein said downloading facilitates a replacement of electronic information stored in said terminal with corresponding decrypted information obtained from decrypting said encrypted information, said downloading system comprising:

(a)   a host device with a host component configured for transmitting said encrypted electronic information therefrom from said host device to said terminal, wherein said encrypted information comprises at least one next version key for later use by said decryption component in decrypting a next version of encrypted electronic information;

(b)   a gaming terminal having said first resident security key and comprising a receiving component configured for receiving said encrypted electronic information by said terminal and a decryption component configured for decrypting said encrypted electronic information; and,

Page 2 of 16

(c)   delivery means configured for separately delivering said ~~other~~ second non-resident security key to said terminal ~~at the time of downloading~~; wherein said downloading of said encrypted electronic information in conjunction with said delivery of said second security key enable a replacement of electronic information stored in said terminal with corresponding decrypted information obtained from said decryption component from decrypting said encrypted electronic information using said resident security key and said delivered non-resident security key.

Claim 2 (original):   A system according to claim 1 wherein said encrypted electronic information is in the form of packs, said packs comprising a full set of files for updating said terminal's software.

Claim 3 (currently amended):   A system according to claim 2 and further comprising a communications link between said host component and said receiving component wherein said communications link comprises a cable coupled to parallel ports of said host component and ~~terminal~~ said receiving component, said receiving component comprising terminal drivers and said host component comprising host drivers; and, wherein said delivery means comprises an electronic security key.

Claim 4 (currently amended):   A system according to claim ~~3~~ 1 wherein said encrypted electronic information comprises at least one next version security key, wherein said first resident key is replaced by said next version key and used by said decryption component in decrypting a next encryption version of electronic information to be received later by said receiving component ~~assigned bit information associated with a next version electronic key, said bit information being for later use with said delivery means to deliver said other security key for use by said decryption component in decrypting a next version of encrypted electronic information~~.

Claim 5 (original):   A system according to claim 4 wherein said cable is wired to

provide crossed control lines and bidirectional communications for data transfer.

Claim 6 (original):   A system according to claim 5 wherein said electronic security
key is configured for providing means for decrypting an encrypted master reset
component in said terminal.

Claim 7 (original):   A system according to claim 6 wherein said electronic security
key comprises information usable by said terminal to distinguish the electronic
information version that different electronic keys are configured for.

Claim 8 (original):   A system according to claim 6 wherein said delivery means
comprises a secure network.

Claim 9 (original):   A system according to claim 8 wherein said network is a wide
area ethernet network.

Claim 10 (original): A system according to claim 4 wherein said files are stored in said
terminal in nonvolatile memory following decryption of said packs.

Claim 11 (cancelled).

Claim 12 (currently amended):   A method for securely downloading encrypted
electronic information from a host device to a gaming terminal, through a
communications link between said host device and said terminal, whereby said terminal
comprises a decryption component configured for decrypting, said encrypted electronic
information being encrypted by using at least two security keys, at least a first one said
key being of said security keys being resident in said terminal and at least another said
a second key of said security keys being non-resident in said terminal and separately
delivered to said terminal apart from said encrypted electronic information being

~~delivered to said terminal at the time of said downloading, and whereby said~~ ~~downloading facilitates a replacement of electronic information stored in said terminal~~ ~~with corresponding decrypted information obtained from decrypting said encrypted~~ ~~information~~, said downloading method comprising:

(a)   transmitting said encrypted electronic information from said host device ~~to said~~ ~~terminal, wherein said encrypted information comprises at least one next version~~ ~~key for later use by said decryption component in decrypting a next version of~~ ~~encrypted electronic information;~~

(b)   receiving said encrypted electronic information at said terminal; and,

(c)   <u>separately</u> delivering said ~~other~~ <u>second non-resident security</u> key to said terminal ~~at the time of downloading~~;

<u>whereby said downloading of said encrypted electronic information in conjunction with said delivery of said second security key enable a replacement of electronic information stored in said terminal with corresponding decrypted information obtained from decrypting said encrypted electronic information using said resident security key and said delivered non-resident security key.</u>

Claim 13 (original): A method according to claim 12 whereby said encrypted electronic information is in the form of packs, said packs comprising a full set of files for updating said terminal's software.

Claim 14 (currently amended):   A method according to claim 13 whereby ~~said~~ ~~communications link comprises a cable coupled to parallel ports of said host and~~ ~~terminal and said~~ delivering comprises providing <u>a physical</u> ~~an~~ electronic security key to said terminal.

Claim 15 (currently amended):   A method according to claim 14 whereby said encrypted <u>electronic</u> information comprises <u>at least one next version security key, whereby said first resident key is replaced by said next version key and used by said</u>

decryption component in decrypting a next encryption version of electronic information to be received later by said receiving component ~~assigned bit information associated with a next version electronic key, said bit information being for later use with said delivery means to deliver said other security key for use by said decryption component in decrypting a next version of encrypted electronic information~~.

Claim 16 (cancelled).

Claim 17 (currently amended):   A method according to claim 15 ~~16~~ and further comprising providing in said electronic security key means for decrypting an encrypted master reset component in said terminal.

Claim 18 (currently amended):   A method according to claim 15 ~~16~~ and further comprising providing in said electronic security key information usable by said terminal to distinguish the electronic information version that different electronic keys are configured for.

Claim 19 (currently amended):   A method according to claim 13 whereby said ~~communications link is a secure network and~~ said delivering is <u>performed</u> ~~performing~~ by means of <u>a secure</u> ~~said~~ network.

Claim 20 (original): A method according to claim 19 whereby said network is a wide area ethernet network.

Claim 21 (new).   A system according to claim 4 wherein said encrypted electronic information comprises assigned bit information associated with at least one next version security key, said bit information being for later use with said delivery means to provide a replacement first resident security key and/or a replacement second non-resident security key to replace one or both of said first resident security key and said second

non-resident security key for use by said decryption component in decrypting a next encryption version of electronic information.

Claim 22 (new):   A method according to claim 15 whereby said encrypted electronic information comprises assigned bit information associated with at least one next version security key, said bit information being for later use with said delivery means to provide a replacement first resident security key and/or a replacement second non-resident security key to replace one or both of said first resident security key and said second non-resident security key for use by said decryption component in decrypting a next encryption version of electronic information.

Appln. No. 09/772,460
Amendment dated: November 8, 2004
Reply to Office Action of August 6, 2004

TITLE AMENDMENT

Please amend the title to read as follows:

System and Method for <u>Securely</u> Downloading Electronic Information to a Video Lottery Terminal.